



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/502,005	07/19/2004	Chin Shyan Ooi	P/2778-50	6804
2352	7590	10/11/2007		
OSTROLENK FABER GERB & SOFFEN			EXAMINER	
1180 AVENUE OF THE AMERICAS			LAFORGIA, CHRISTIAN A	
NEW YORK, NY 100368403				
			ART UNIT	PAPER NUMBER
			2131	
			MAIL DATE	DELIVERY MODE
			10/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

QH

Office Action Summary	Application No.	Applicant(s)	
	10/502,005	OOI ET AL.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 10 August 2007.
 2a) This action is **FINAL**. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-20 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-20 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on 09 July 2004 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) <input type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)	5) <input type="checkbox"/> Notice of Informal Patent Application
Paper No(s)/Mail Date _____	6) <input type="checkbox"/> Other: _____

DETAILED ACTION

1. The amendment of 10 August 2007 has been noted and made of record.
2. Claims 1-20 have been presented for examination.
3. Claims 21 and 22 have been cancelled as per Applicant's request.

Response to Arguments

4. Applicant's amendments, see page 2, filed 10 August 2007, with respect to the abstract and specification have been fully considered and are persuasive. The objections of the abstract and specification have been withdrawn.
5. Applicant's arguments regarding the prior art rejection of claims 1-20 filed 10 August 2007 have been fully considered but they are not persuasive.
6. The Examiner disagrees with the Applicant's assertions on page 9 that Wang does not disclose a cryptoprogram stored in read-only memory. As the Applicant notes on page 9, the Examiner draws the cryptogram to Wang's disclosed authentication algorithm and the read-only memory to Wang's system memory. The Applicant argues that a skilled artisan would not have recognized that the system memory could have been a read-only memory. The Examiner disagrees with this allegation, since a skilled artisan would have recognized that there were only a finite number of solutions for the system memory at the time the invention was made, one such solution being a read-only memory. See *KSR International Co. v. Teleflex Inc.*, 82 USPQ2d 1385 (U.S. 2007).
7. Therefore it would have been possible for one of ordinary skill in the art to pursue a read only memory to store the authentication algorithm since a read only memory would prevent

someone from overwriting or corrupting the authentication algorithm and the rejection of independent claim 1 has been maintained.

8. The Examiner disagrees with the Applicant's disclosure that Wang does not teach the use of a microcontroller to execute an authentication algorithm stored in a read-only memory. As discussed above, Wang discloses an authentication algorithm (i.e. cryptoprogram) stored in a read-only memory (i.e. system memory, that one of ordinary skill would recognize could be read-only memory). The Examiner cited Figure 1, element 22 (i.e. the processor) as representing the Applicant's claimed microcontroller. The processor of Wang clearly executes the instructions stored in system memory (figure 1, element 20), which includes, but is not limited to, the cryptoprogram.

9. The Examiner disagrees with the Applicant's arguments on page 9 that Wang does not disclose an authentication algorithm to verify the password with the authentication sequence. The Applicant attempts to misrepresent Wang in stating that a password is matched to a stored password without the execution of an authentication algorithm. Wang discloses that a user inputs a password using a keyboard (column 2, lines 39-41) and that the cryptoprogram searches for a corresponding password in the programmable memory of the key (column 2, lines 41-53). As such Wang teaches the Applicant's claimed an authentication algorithm (i.e. the cryptoprogram) to verify the password (column 2, lines 39-41, i.e. the inputted password) with the authentication sequence (i.e. stored password).

10. Since Wang has been shown to teach the Applicant's claimed an authentication algorithm to verify the password with the authentication sequence, the rejection of independent claim 1 has been maintained.

11. The Examiner disagrees with the Applicant's arguments, on page 10, that the system memory of Wang cannot both be the read-only memory unit to store an authentication algorithm and a second storage unit to store data from the web server. The Applicant argues that the read only memory and the second storage unit are separate units (page 10, first paragraph, last sentence), yet the claim language makes no such distinction. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Therefore, until such a time that the Applicant's clarify the claim language that the first and second storage units are separate and distinct storage units, the Examiner shall continue to construe the storage units as a single unit with multiple memory units for storing a multitude of information.

12. Furthermore, it is clear that system memory contains the authentication algorithm (i.e. cryptoprogram) from figure 1. As cited in the previous action, as well as again below, Wang makes it clear at column 1, lines 32-33 that the system memory also stores programs and files. Thereby showing that the system memory stores the cryptoprogram (i.e. Applicant's claimed authentication algorithm) and data. Wang does not teach the origin of the data, and the Examiner relies on Elteto to provide a teaching of obtaining data via a web server. The Applicant's arguments with regards to Elteto amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

13. Since it has been shown that the combination of Wang and Elteto teach all the limitations of claim 1, the rejection is maintained.

14. The Applicant essentially reiterates the arguments of claim 1 in his arguments regarding claim 18 on pages 11-13. As such, the rejection of independent claim 18 is maintained for the reasons argued above.

15. The Examiner disagrees with the applicant's argument regarding claims 10 and 11 that Wang does not teach an encoder and decoder for encrypting and decrypting, respectively. If the prior art structure is capable of performing the intended use, in this case the respective encrypting and decrypting, then it meets the claim. Therefore the rejection of claims 10 and 11 is maintained.

16. In response to applicant's argument on page 14 that Elteto's use of hashes is different from that of the instant invention, a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, in this case performing hash coding on the second storage unit, then it meets the claim. The Applicant has failed to show that there is a structural difference that distinguishes the instant invention from the prior art.

17. The Examiner disagrees with the Applicant's allegation that the first storage unit is not read-only memory. As point out in the previous Office action, as well as again below, Wang states at column 2, lines 16-18, that the first storage unit (i.e. the memory of the key **18**) is an EEPROM, or electronically erasable programmable read only memory. Therefore, Wang discloses wherein the first storage unit is read-only memory in disclosing that the memory is an EEPROM. Since the memory is an EEPROM, the stored passwords must be hard-coded into the memory. Wang teaches a first storage unit is a read-only memory unit and that the

authentication sequence (i.e. passwords) are hard-coded in disclosing the memory of the security key is an EEPROM, therefore the rejection of claim 15 is maintained.

18. Applicant's arguments regarding claims 16 and 17 fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. The Applicant merely states that the items the Examiner pointed to are not the same as the Applicant's instant invention without specifically pointing out how the language of the claims patentably distinguishes them from the cited prior art. Furthermore, the Applicant has failed to show that there is a structural difference that distinguishes the instant invention from the prior art.

19. Applicant's arguments regarding claim 2 fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. The Applicant merely states that the items the Examiner pointed to are not the same as the Applicant's instant invention without specifically pointing out how the language of the claims patentably distinguishes them from the cited prior art.

20. The Examiner disagrees with the Applicant's misrepresentation of Miller as it pertains to claim 3. Miller discloses returning a computer to sleep mode after a certain number of failed password attempts as cited in the previous office action, and again below. A skilled artisan would have recognized that there were only a finite number of solutions for taking action after a certain number of failed passwords at the time the invention was made, such as forcing the computer to a sleep mode or shutdown or locking the computer. See *KSR International Co. v.*

Teleflex Inc., 82 USPQ2d 1385 (U.S. 2007). One of ordinary skill in the art would recognize that shutting down a computer and putting it to sleep produce the same result, namely that the unauthorized user who entered X number of improper passwords is denied access.

21. In response to applicant's argument on page 17 regarding claim 4 that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies, such as how the keys are distributed, are not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The claim merely requires that the password is received from a web server. Elteto discloses a system that distributes keys, which are drawn to the applicant's claimed password, that are transmitted from a central key depository, which can be construed as the Applicant's claimed web server. Therefore, the combination of Wang and Elteto teach the limitations of claim 4 and the rejection is maintained.

22. The Examiner disagrees with the Applicant's arguments on page 17 with regards to claim 5. Wang clearly shows that the cryptoprogram (i.e. authentication algorithm) is embedded in the system memory, thereby being hard-coded in firmware and hardware. As such the rejection of claim 5 is maintained.

23. In response to the Applicant's arguments on pages 17 and 18 regarding claims 6 and 7, the Examiner disagrees. Technically any form of system memory may be removable, from a hard drive to flash memory. They are all portable depending on the tools handy. Therefore, the rejection of claims 6 and 7 is maintained.

24. Applicant's arguments regarding claim 14 fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

25. See further rejections that follow.

Claim Rejections - 35 USC § 103

26. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

27. Claims 1, 10-12, and 15-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,618,807 to Wang et al., hereinafter Wang, in view of U.S. Patent No. 7,111,324 to Elteto et al., hereinafter Elteto.

28. As per claim 1, Wang teaches an authentication system to verify a password, the system being arranged for coupling to a host for communication therewith, and comprising:

a first storage unit to store an authentication sequence (Figure 1 [block 30], column 2, lines 61-65, i.e. storing the password in the electronic key);

a read-only memory unit to store an authentication algorithm (Figure 1 [block 26], column 1, lines 42-48, i.e. the crypto program performing password authentication);

a microcontroller (Figure 1 [block 22]) coupled to said first storage unit (Figure 1 [block 28]) and said read-only memory unit (Figure 1 [block 20]), wherein said microcontroller is to receive said password and execute said authentication algorithm and wherein said authentication algorithm is to verify said password with said authentication sequence (column 2, lines 38-54, i.e. user inputs password and the crypto program searches for the appropriate password); and

a second storage unit coupled to said microcontroller to store data (Figure 1 [block 20], column 1, lines 32-33, i.e. system memory for storing programs and files) and wherein access to said second storage unit is permitted by said microcontroller only if said password has been verified (column 2, lines 38-54, i.e. if the inputted password matches the previously entered password, the program or file is decrypted).

and decrypting data that has previously been encrypted before use thereof in the host (column 2, lines 38-54, i.e. if the inputted password matches the previously entered password, the program or file is decrypted).

29. Wang does not disclose wherein the system memory is read only memory.

30. One of ordinary skill in the art would recognize that there are only a finite number of solutions for the disclosed system memory, which include but are not limited to, read only memory (ROM, random access memory (RAM), and other such non-volatile memory, such as hard disks and optical disks. Since there are only a limited number of possible solutions for Wang's disclosed system memory, it would have been possible for one of ordinary skill in the art to pursue a read only memory to store the authentication algorithm since a read only memory would prevent someone from overwriting or corrupting the authentication algorithm. See *KSR International Co. v. Teleflex Inc.*, 82 USPQ2d at 1393-1397 (U.S. 2007).

31. Wang does not disclose a web server and wherein the system is arranged to receive data from the web server, via the host.

32. Elteto teaches a web server (Figures 1, 2, 7, and 8 [block 134]) and wherein the system is arranged to receive data from the web server (column 4, lines 35-62, column 7, lines 37-50, i.e. encrypting files, remotely accessing files).

33. It would have been obvious to one of ordinary skill in the art at the time the invention was made to receive encrypted data from a web server, since Elteto states at column 4, lines 2-4 that encrypting files that are transmitted from a remote server implements software protection schemes to prevent copying and unauthorized use of those files, thereby deterring software piracy and hackers from gaining access to said files.

34. Regarding claim 10, Wang teaches an encoder coupled between said microcontroller and said second storage unit, wherein said encoder is to encrypt data that is to be written onto said second storage unit (column 1, lines 35-36, column 2, lines 29-38, i.e. encrypting the program or file).

35. With regards to claim 11, Wang teaches a decoder coupled between said microcontroller and said second storage unit, wherein said decoder is to decrypt data that is to be read from said second storage unit (column 1, lines 35-36, column 2, lines 44-53, i.e. decrypting the program or file).

36. Concerning claim 12, Elteto discloses wherein data stored in said second storage unit is hash-coded (Figures 3 [blocks 302, 304, 306], 4 [block 410], column 8, lines 19-39, column 8, line 53 to column 9, line 8).

37. Regarding claim 15, Wang teaches wherein said first storage unit is located within said read-only memory unit (Figure 1 [block 28], column 2, lines 14-28) and wherein said

authentication sequence is hard coded into said first storage unit (Figure 1 [block 30], column 2, lines 14-28).

38. With regards to claim 16, Elteto teaches wherein said second storage area further comprises a public storage area (Figure 3 [block 324]) and a private storage area (Figure 3 [block 326]).

39. Concerning claim 17, Wang and Elteto do not teach wherein said first storage unit is located within said private storage area of said second storage area.

40. It would have been obvious to one of ordinary skill in the art at the time the invention was made have the first storage unit be located within the private storage area of the second storage unit, since one of ordinary skill in the art would recognize that by having the first storage unit, which contains the encrypted password, part of the private section of the second storage area it would be more difficult for an unauthorized user to gain access to the owner of the electronic key's password.

41. As per claim 18, Wang teaches a method for authenticating a password, comprising:
coupling an authentication system to a host for communication therewith (column 2, lines 14-28, i.e. electronic key can be inserted);
the system receiving said password (column 2, lines 38-54, i.e. user inputs password);
the system providing an authentication sequence (Figure 1 [block 30], column 2, lines 61-65, i.e. storing the password in the electronic key);

the system executing an authentication algorithm (Figure 1 [block 26]) to verify said password with said authentication sequence (column 2, lines 38-54, i.e. user inputs password and the crypto program searches for the appropriate password), wherein said authentication algorithm is stored on a read-only memory unit of the system (Figure 1 [block 26]);

the system permitting access to said data on said storage unit only if said password is verified (column 2, lines 38-54, i.e. if the inputted password matches the previously entered password, the program or file is decrypted); and

the system decrypting the data before use in the host (column 2, lines 38-54, i.e. if the inputted password matches the previously entered password, the program or file is decrypted).

42. Wang does not disclose wherein the system memory is read only memory.

43. One of ordinary skill in the art would recognize that there are only a finite number of solutions for the disclosed system memory, which include but are not limited to, read only memory (ROM, random access memory (RAM), and other such non-volatile memory, such as hard disks and optical disks. Since there are only a limited number of possible solutions for Wang's disclosed system memory, it would have been possible for one of ordinary skill in the art to pursue a read only memory to store the authentication algorithm since a read only memory would prevent someone from overwriting or corrupting the authentication algorithm. See *KSR International Co. v. Teleflex Inc.*, 82 USPQ2d at 1393-1397 (U.S. 2007).

44. Wang does not disclose the system receiving data from a web server, via the host, in encrypted form, wherein said data is stored in a storage unit of the system.

45. Elteto teaches the system receiving data from a web server, via the host, in encrypted form, wherein said data is stored in a storage unit of the system (column 4, lines 35-62, column 7, lines 37-50, i.e. encrypting files, remotely accessing files).

46. It would have been obvious to one of ordinary skill in the art at the time the invention was made to receive encrypted data from a web server, since Elteto states at column 4, lines 2-4 that encrypting files that are transmitted from a remote server implements software protection schemes to prevent copying and unauthorized use of those files, thereby deterring software piracy and hackers from gaining access to said files.

47. Regarding claim 19, Elteto teaches wherein said password is received from said web server (column 7, lines 37-49, i.e. keys are distributed from a central key to grant access to private documents).

48. With regards to claim 20, Wang discloses wherein said password is entered by a user (column 2, lines 38-54).

49. Claims 2-9 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wang in view of Elteto as applied to claim 1 above, and further in view of U.S. Patent No. 6,038,320 to Miller, hereinafter Miller.

50. Regarding claim 2, Wang and Elteto do not teach wherein the password is received by said microcontroller from said host.

51. Miller teaches wherein the password is received by said microcontroller from said host (Figure 8 [block 320], column 5, lines 54-64).

52. It would have been obvious to one of ordinary skill in the art at the time the invention was made to transmit the password from the host to the microcontroller, since Miller states at column 3, lines 57-67 that by sending the password to an inappropriate security key prevents unauthorized users from accessing the system since the authorized key codes do not match (column 4, lines 47-62), thereby only allowing user's in possession of the security key that contains their password access to the system.

53. With regards to claim 3, Miller teaches a shutdown algorithm to shut down said host and said authentication system after a number of incorrect passwords is received by said microcontroller (Figure 8 [block 300], column 5, lines 1-9, column 5, lines 53-64). A skilled artisan would have recognized that there were only a finite number of solutions for taking action after a certain number of failed passwords at the time the invention was made, such as forcing the computer to a sleep mode or shutdown or locking the computer. See *KSR International Co. v. Teleflex Inc.*, 82 USPQ2d 1385 (U.S. 2007). One of ordinary skill in the art would recognize that shutting down a computer and putting it to sleep produce the same result, namely that the unauthorized user who entered X number of improper passwords is denied access.

54. With regards to claim 4, Elteto teaches wherein said password is received by said host from said web server (column 7, lines 37-49, i.e. keys are distributed from a central key to grant access to private documents).

55. With regards to claim 5, Wang teaches wherein said authentication algorithm is hard coded on one of a group consisting of a firmware and a hardware in said microcontroller (Figure 1 [block 26], column 2, lines 1-14, column 2, lines 29-64).

56. Concerning claim 6, Wang teaches wherein said second storage unit is a removable storage device (Figure 1 [blocks 18, 28], column 2, lines 14-28).

57. Concerning claim 7, Wang discloses wherein said second storage unit uses flash memory (Figure 1 [blocks 28], column 2, lines 14-28).

58. With regards to claim 8, Wang, Elteto, and Miller all disclose security/electronic keys comprising a USB interface. Elteto illustrates wherein said microcontroller and said read-only memory unit are implemented on a single semiconductor chip in at least figure 2 and column 6, line 60 to column 7, line 9 and column 14, lines 10-33. Figures 2, 4a-c, and 6a-f of U.S. Patent No. 6,848,045 provide even more illustration of the inner workings of the devices disclosed in Wang, Elteto, and Miller, thereby showing that the USB security keys have a microcontroller and memory unit implemented on a single semiconductor chip. This is further supported by figure 1 of Applicant's own patents 6,880,054 and 7,039,759, which clearly shows that USB security keys with a microcontroller and memory unit implemented on a single semiconductor chip was known as early as 2001.

59. Concerning claim 9, Wang, Elteto, and Miller all disclose security/electronic keys comprising a USB interface. Elteto teaches wherein said first storage unit and said read-only memory unit are incorporated into said microcontroller in at least figure 2 and column 6, line 60 to column 7, line 9 and column 14, lines 10-33. Figures 2, 4a-c, and 6a-f of U.S. Patent No. 6,848,045 provide even more illustration of the inner workings of the devices disclosed in Wang, Elteto, and Miller, thereby showing that the USB security keys have a microcontroller that incorporates a first storage unit and read-only memory. This is further supported by figure 1 of Applicant's own patents 6,880,054 and 7,039,759, which clearly shows that USB security keys have a microcontroller that incorporates a first storage unit and read-only memory was known as early as 2001.

60. Concerning claim 13, Wang and Elteto do not teach wherein said authentication sequence is encrypted.

61. Miller discloses wherein said authentication sequence is encrypted (Figure 4B [block 76], 5 [block 94], 8 [block 340], column 3, lines 47-51, column 4, lines 28-30, column 5, lines 1-9, column 5, lines 53-64).

62. It would have been obvious to one of ordinary skill in the art at the time the invention was made to encrypt the stored password, since one of ordinary skill in the art would realize that, if the security key was ever stolen or came into the possession of an unauthorized user, an encrypted password would provide additional security since any unauthorized users would first have to decrypt the stored password in order to gain access to the user's accounts.

63. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wang in view of Elteto as applied to claim 12 above, and further in view of U.S. Patent 6,178,508 to Kaufman, hereinafter Kaufman.

64. Concerning claim 14, Wang and Elteto do not teach wherein said authentication sequence is hash-coded.

65. Kaufman discloses wherein said authentication sequence is hash-coded (Abstract, column 2, lines 27-46).

66. It would have been obvious to one of ordinary skill in the art at the time the invention was made to store a hashed password, since Kaufman states at column 2, lines 35-38 that hashing the password prevents the password from being recreated by an unintended party, thereby providing additional security since any unauthorized users that came into possession of the security key would not be able to gain access to the stored password, which prevents the unauthorized user from gaining access to the user's accounts.

Conclusion

67. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

68. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

69. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

70. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

71. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131



clf